

1 JOHN M. NEUKOM (CA Bar No. 275887)
johnneukom@quinnemanuel.com
2 ANDREW M. HOLMES (CA Bar No. 260475)
drewholmes@quinnemanuel.com
3 ALICIA VEGLIA (CA Bar No. 291070)
aliciaveglia@quinnemanuel.com
4 QUINN EMANUEL URQUHART & SULLIVAN, LLP
50 California Street, 22nd Floor
5 San Francisco, California 94111
Telephone: (415) 875-6600
6 Facsimile: (415) 875-6700

7 Attorneys for Plaintiff FORTINET, INC.

8
9 **UNITED STATES DISTRICT COURT**
10 **NORTHERN DISTRICT OF CALIFORNIA**
11 **SAN FRANCISCO DIVISION**

12 Case No. 3:13-cv-05831-LB

13
14
15 FORTINET, INC., a corporation,
16
17 Plaintiff,

18 vs.

19 SOPHOS, INC., a corporation,
MICHAEL VALENTINE, an individual,
20 and JASON CLARK, an individual,
21 Defendants.
22
23
24

**FORTINET, INC.’S FIRST AMENDED
COMPLAINT FOR
(1) PATENT INFRINGEMENT,
(2) TRADE SECRET
MISAPPROPRIATION,
(3) BREACH OF CONTRACT,
(4) BREACH OF IMPLIED
COVENANT OF GOOD FAITH AND
FAIR DEALING,
(5) INTENTIONAL INTERFERENCE
WITH CONTRACT,
(6) CIVIL CONSPIRACY,
(7) BREACH OF FIDUCIARY DUTIES,
(8) AIDING AND ABETTING BREACH
OF FIDUCIARY DUTIES, AND
(9) VIOLATION OF CAL. BUS. &
PROF. CODE § 17200 *ET SEQ.*—
UNFAIR COMPETITION**

DEMAND FOR JURY TRIAL

1 Plaintiff Fortinet, Inc. (“Fortinet”) hereby alleges for its First Amended Complaint against
2 Defendants Sophos, Inc. (“Sophos”), Michael Valentine (“Valentine”), and Jason Clark (“Clark”)
3 on personal knowledge as to its own actions and on information and belief as to the actions of
4 Sophos, Valentine, Clark and third parties as follows:

5 **INTRODUCTION**

6 1. Fortinet brings this action against Sophos, Valentine, and Clark to seek remedies
7 for the repeated and ongoing violations of Fortinet’s legal rights. This includes Sophos’ trade
8 secret misappropriation as well as infringement of United States Patent Nos. 7,698,744; 8,069,487;
9 8,195,938; 7,333,430; 7,376,125; and 7,609,625 (collectively, the “Asserted Patents”). This also
10 includes the wrongful conduct of Sophos, Valentine, and Clark with respect to Fortinet’s
11 intellectual property, contractual, statutory, and common-law entitlements.

12 2. Fortinet is a publicly-traded, world-wide leading provider of network security
13 solutions and unified threat management. Sophos is a private company; a less-prominent provider
14 of network security solutions that—as compared to Fortinet—are often considered “entry level”;
15 and a competitor of Fortinet.

16 3. Sophos has recently conducted—and to this day continues to pursue—an unusually
17 brazen and unusually widespread attempt to unlawfully poach Fortinet’s patented technologies and
18 trade secrets, and to solicit Fortinet employees to terminate their relationships with Fortinet and
19 breach their contracts with Fortinet. Sophos has undertaken this campaign in hopes of improving
20 its relatively weak competitive position in the market, and to hurt the business of Fortinet.

21 4. This conduct by Sophos is taking the form of patent infringement and trade secret
22 misappropriation. That conduct is being bolstered—unlawfully—pursuant to an ongoing and at
23 this point egregious campaign to “raid” Fortinet’s employees, trade secrets, and patented
24 technology.

25 5. Fortinet champions the benefits that individual employees bring to a business.
26 Fortinet furthermore respects the rights of individuals to seek employment freely under California
27 law, and California laws protecting employee mobility. As such, Fortinet does not base its causes
28 of action on the repeated decisions of Sophos to hire individuals who have worked at Fortinet.

1 Rather, Fortinet takes issue with—*inter alia*—the repeated decisions by Sophos, Valentine, and
2 Clark to (i) use in improper and unlawful fashion the knowledge (including of Fortinet’s trade
3 secrets) and contacts of Valentine, Clark, and other Fortinet employees (former and current) in
4 Sophos’ efforts to intentionally interfere with Fortinet’s relationships with its own employees, and
5 (ii) violate numerous, enforceable contracts which provide that former Fortinet employees should
6 not, for a short and reasonable period of time, encourage or solicit other Fortinet employees to
7 terminate their employment with Fortinet. This campaign is unlawful, designed to harm Fortinet’s
8 business and employee relationships, and does not represent fair play.

9 6. Sophos’ unlawful conduct is furthermore unusually widespread—spanning
10 numerous patents, trade secrets of numerous categories, and affecting numerous current and
11 former employees.

12 7. To wit: Fortinet does not bestow the title of “Vice President” widely. For a
13 company with over 2,200 employees, Fortinet maintains a modest number of unusually important
14 employees whom are given the “Vice President” title. These Vice Presidents are Fortinet’s
15 executives; they owe Fortinet fiduciary duties; they manage substantial teams of employees; and
16 they are responsible for setting and executing Fortinet’s business objectives in a competitive
17 market.

18 8. Sophos has nonetheless executed an all-out assault on Fortinet’s team of Vice
19 Presidents. Sophos has already successfully convinced four Fortinet Vice Presidents to leave
20 Fortinet—Fortinet’s former Vice Presidents for Americas Sales; Channel Sales; North America
21 Distribution; and Systems Engineering. Sophos has further attempted—unsuccessfully—to lure
22 two additional Fortinet Vice Presidents to leave Fortinet—Fortinet’s Vice President for Marketing
23 and another of Fortinet’s highest-ranking Vice Presidents.

24 9. Sophos’ unlawful conduct is furthermore systematic and appears to represent a
25 deliberate corporate decision by Sophos. Sophos has abused Fortinet’s intellectual property and
26 contractual entitlements in part by using Fortinet’s trade secrets to solicit numerous Fortinet Vice
27 Presidents and other important personnel, over almost a year’s time, including as recently as *after*

1 Fortinet filed its initial complaint in this case. Sophos' CEO has recently and publicly endorsed
2 this Sophos conduct.

3 10. And Sophos' unlawful conduct has furthermore been brazen. In response to
4 Fortinet's initial complaint, Sophos's CEO gave 1–2 interviews to the press, insulting this lawsuit.
5 Sophos' CEO furthermore authored a web blog further insulting the lawsuit and inviting
6 applications to work at Sophos. Sophos' and Clark's conduct has even intensified since the filing
7 of the initial complaint, with increasing attempts to interfere with Fortinet's relationships with its
8 own employees in recent weeks.

9 11. Fortinet asks that Sophos and Valentine and Clark be ordered to stop this conduct
10 and to remedy the wrongs that Sophos seems so intent on inflicting on Fortinet. Sophos' desire—
11 as a private company with entry-level products and without substantial traction in the network
12 security markets, as compared to Fortinet—to improve its own business is understandable. But
13 Sophos' means for doing so are not.

14 **PARTIES**

15 12. Fortinet is a Delaware corporation with a principal place of business at 1090 Kifer
16 Road, Sunnyvale, California 94086. Fortinet is a leading provider of network security appliances
17 and services, and a market leader in unified threat management systems.

18 13. Defendant Sophos is a Massachusetts corporation having its principal place of
19 business in the United States at 3 Van de Graaff Drive, Second Floor, Burlington, Massachusetts
20 01803.

21 14. Defendant Valentine is an individual who was previously employed by Fortinet,
22 and is now employed by Sophos as the "Senior Vice President, Worldwide Sales" of Sophos, as
23 alleged in greater detail below. Valentine lives and works in this District. On information and
24 belief, Valentine maintains his primary residence in Los Gatos, California.

25 15. Defendant Jason Clark is an individual who was previously employed by Fortinet,
26 and is now employed by Sophos as the "Director of Sales Engineering," as alleged in greater detail
27 below. On information and belief, Clark maintains his primary residence and/or works physically
28 in the Dallas / Fort Worth area of Texas.

1 **JURISDICTION AND VENUE**

2 16. This is an action for patent infringement arising in part under the patent laws of the
3 United States, codified at 35 U.S.C. §§ 1, *et seq.* This Court has subject matter jurisdiction over
4 this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5 17. This Court has supplemental jurisdiction over Fortinet’s state law claims pursuant
6 to 28 U.S.C. § 1367. The federal and state claims alleged herein are so related that they form part
7 of the same case or controversy. Examples (not comprehensive) of the relation of patent versus
8 non-patent claims include the following: Sophos’ campaign to misappropriate Fortinet’s
9 intellectual property includes patents and trade secrets alike; Sophos’ campaign to misappropriate
10 Fortinet’s intellectual property, including patented and non-patented intellectual property, applies
11 to an overlapping set of competitive products; damages for Fortinet’s patent and non-patent claims
12 will require inquiry into facts regarding development, marketing and sales of numerous
13 overlapping, competitive products. Judicial economy, convenience, and fairness to the parties will
14 result if this Court asserts jurisdiction over the state claims.

15 18. This Court has personal jurisdiction over Sophos. On information and belief,
16 Sophos has transacted business in this District, contracted to supply goods or services in this
17 District directly or through its agents, has offered for sale, sold and/or advertised its products and
18 services in the this District, and has otherwise purposely availed itself of the privileges and
19 benefits of the laws of the State of California. In addition, this Court has jurisdiction over Sophos
20 because Sophos has committed acts of patent infringement during the course of its business in this
21 District. In addition, as alleged below, Sophos currently employees 1+ individuals in this District
22 and is therefore physically present here, has poached 1+ individuals in this District from the
23 employment of Fortinet, and has induced 1+ individuals in this District to breach contractual
24 agreement(s) with Fortinet. Furthermore, Sophos maintains systematic, ongoing business
25 operations inside this District, including a physical presence inside this District. By way of
26 example, Sophos has recently listed numerous job openings inside this District on its own web
27 site, including an opening for a “Channel Manager – West Coast” with a “Location” defined as
28 “Santa Clara, California.” Sophos has recently advertised a job opening for an “Enterprise

1 Account Executive – Northern California” with a “Location” defined as “San Francisco,
2 California.” Sophos has recently advertised a job opening for an “Office Administrator” with a
3 “Location” defined as “Santa Clara, California,” and with a job description that indicates that
4 Sophos maintains at least one permanent office inside this District, given that the “Main Duties”
5 include “Greeting and directing visitors” and “Issuing visitor badges.” Furthermore, according to
6 recent news reports, Sophos now maintains a physical office inside this District, where Sophos’
7 CEO works. See [http://channelnomics.com/2014/01/08/sophos-officially-opens-silicon-valley-](http://channelnomics.com/2014/01/08/sophos-officially-opens-silicon-valley-office/)
8 [office/](http://channelnomics.com/2014/01/08/sophos-officially-opens-silicon-valley-office/) (last visited Jan. 8, 2014). According to the web site for the California Secretary of State,
9 Sophos has a California business entity number, and maintains an agent for service of process
10 inside California.

11 19. This Court has personal jurisdiction over Valentine because he maintains his
12 primary residence in this District, and because he has intentionally and repeatedly engaged in
13 conduct—which forms the basis for Fortinet’s claims against Valentine—to harm Fortinet here
14 inside this District. Valentine furthermore now works for Sophos in an office located inside this
15 District. See <http://channelnomics.com/2014/01/08/sophos-officially-opens-silicon-valley-office/>
16 (“ . . . Mike Valentine will work primarily or part-time from this facility.”) (last visited Jan. 8,
17 2014).

18 20. This Court has personal jurisdiction over Clark because Clark has intentionally,
19 expressly and repeatedly engaged in conduct—which forms the basis for Fortinet’s claims against
20 Clark—to harm Fortinet, which as Clark knows maintains its principal place of business here
21 inside this District. Clark intentionally misused confidential and trade secret Fortinet information
22 and breached a contract with Fortinet, and induced others to breach contracts with Fortinet,
23 knowing and intending that the harms suffered by Fortinet as a result of that conduct and those
24 breaches would occur here in this District. Clark furthermore, on information and belief, accessed
25 and then misused trade secret information belonging to Fortinet, which information Fortinet has
26 developed and safeguards inside this District, further intentionally inflicting harm on a company
27 based in this District. Clark furthermore, on information and belief, engaged in conduct which
28 forms the basis for Fortinet’s claims inside this District, for example by directing communications

1 to this District (to Sophos, Valentine and others) and—on information and belief—by physically
2 appearing inside this District to further his efforts at breach of contract.

3 21. Venue is proper in this District pursuant to 28 U.S.C. § 1400(b) and 28 U.S.C.
4 § 1391.

5 **INTRADISTRICT ASSIGNMENT**

6 22. This is an intellectual property action exempt from intradistrict assignment under
7 Civil Local Rule 3-2(c), which makes this action subject to assignment on a district-wide basis.

8 **FACTUAL BACKGROUND**

9 23. Founded in 2000, and publicly traded starting in 2009, Fortinet is a leader and
10 worldwide provider of innovative network security appliances and unified threat management
11 solutions. Fortinet's products and subscription services provide broad, integrated and high-
12 performance protection against security threats while simplifying IT security infrastructures.
13 Fortinet is a pioneer in the creation of Unified Threat Management ("UTM") security systems,
14 which enable secure business communications. Fortinet's "Fortigate" systems detect and
15 eliminate the most damaging, content-based threats from email and web traffic without degrading
16 network performance. By integrating the industry's broadest suite of security protections,
17 Fortigate systems allow Fortinet customers to obtain the most comprehensive UTM solutions.
18 Fortinet is now the world's leading provider of UTM security systems, with over 20,000
19 customers worldwide. Fortinet is headquartered in Sunnyvale, California, with customer support,
20 development, and sales facilities located throughout the world.

21 24. Fortinet has expended substantial resources researching and developing its patented
22 technologies, trade secrets, technical strategies, employee relationships, actual and potential
23 customer relationships, actual and potential partner relationships, and business plans related to its
24 security products and services. Fortinet has done so through the expenditure of considerable
25 employee work hours and company resources. These efforts have led to numerous innovative
26 products in the network security market. The United States Patent and Trademark Office has
27 recognized Fortinet's achievements by awarding numerous patents to Fortinet and its inventors as
28 a result of these innovations.

1 25. Fortinet has likewise expended substantial resources in recruiting, hiring, training
2 and retaining its personnel.

3 26. On information and belief, Sophos competes with Fortinet in the network security
4 industry.

5 **Michael Valentine's Tenure at Fortinet**

6 27. For a period of almost six years—from May 2007 until February 2013—Valentine
7 served as an officer and senior executive at Fortinet. His title at Fortinet was “Vice President
8 Americas - Sales and Support.” Valentine occupied the highest possible executive management
9 position for a sales and service function at Fortinet.

10 28. Valentine was one of the highest ranking officers and executives at Fortinet, and
11 supervised a large team of employees. Fortinet maintained a profile for Valentine on its public
12 web site, identifying Valentine as a key member of Fortinet's “Executive Management.”

13 29. Valentine reported to Fortinet's Founder, Chairman of the Board and CEO.
14 Valentine met with the board of directors of Fortinet in his capacity as a senior executive of the
15 company. Valentine was responsible for supervising a large team of sales and support employees
16 of Fortinet, both domestically and internationally.

17 30. While Valentine served as an officer and senior executive of Fortinet, he was
18 provided substantial compensation by Fortinet.

19 31. Valentine's duties at Fortinet from 2007 to 2013 have recently been described by
20 Valentine and/or Sophos on the public web site for Sophos as follows:

21 . . . With more than twenty years of senior sales and channel
22 experience at global IT security companies, Michael most recently
23 served as vice president, Americas sales and support at Fortinet. In
24 this role, ***he oversaw all facets of the company's network security***
25 ***offerings—VPN, UTM, web filter, security software—and business***
26 ***development across North America, Latin America and***
27 ***Australia/New Zealand***, helping to increase corporate revenues by
28 nearly 40 percent.

26 ***He guided Fortinet's multi-national sales team through the***
27 ***company's successful IPO and played a major role in the***
28 ***integration of two acquired companies' sales teams.*** During his
tenure, ***he also expanded the company's network of North America***

1 *technology distributors, signed more than 700 new Americas*
2 *partners and grew the internal channel team by more than 80*
3 *percent, ultimately helping the company grow from \$200 million to*
 over \$500 million in worldwide annual revenue.

4 He is a recognized and respected sales executive who in 2008 and
5 2009 was named a top “Channel Chief” by CRN magazine. . . .

6 See <http://www.sophos.com/en-us/company/management/michael-valentine.aspx> (last visited Dec.
7 16, 2013, emphasis added).

8 32. When Valentine began his duties at Fortinet, in exchange for good and valuable
9 consideration, he chose to execute a written agreement with Fortinet (“Valentine Agreement”).
10 Valentine chose to sign the Agreement on May 21, 2007. A copy of the Agreement, signed by
11 Valentine, is attached hereto as ***Exhibit A***.

12 33. In executing the Valentine Agreement on May 21, 2007, Valentine agreed to a
13 clause with the title “Solicitation of Employees.” Valentine agreed as follows:

14 I agree that *for a period of twelve (12) months immediately*
15 *following the termination of my relationship with the Company* for
16 any reason, whether voluntary or involuntary, with or without cause,
17 ***I shall not either directly or indirectly solicit any of the Company’s***
 employees to leave their employment, or attempt to solicit
 employees of the Company, either for myself or for any other person
 or entity.

18 See Exhibit A at ¶ 8 (emphasis added).

19 34. In executing the Valentine Agreement on May 21, 2007, Valentine also agreed to a
20 clause with the title “Confidential Information.” Valentine agreed as follows: “I agree at all times
21 during my employment with the Company and thereafter, to hold in the strictest confidence, and
22 not to use . . . or to disclose to any person . . . any Company Confidential Information.” See
23 Exhibit A at ¶ 2.A.

24 35. In executing the Valentine Agreement on May 21, 2007, Valentine also agreed to a
25 clause with the title “Termination Certification.” Valentine agreed as follows:

26 ***Upon separation from employment with the Company, I agree to***
27 ***immediately sign and deliver to the Company the “Termination***
 Certification” attached hereto as Exhibit C. I also agree to keep the
28 Company advised of my home and business address for a period of

1 three (3) years after termination of my employment with the
2 Company, so that the Company can contact me regarding my
continuing obligations provided by this Agreement.

3 See Exhibit A at ¶ 6 (emphasis added).

4 36. Valentine chose to leave Fortinet in February 2013.

5 37. When Valentine chose to leave Fortinet in February 2013, he abided by the
6 requirement in the Valentine Agreement that he execute a Termination Certification
7 (“Certification”). Valentine signed his Certification on February 25, 2013. A copy of the
8 Certification, signed by Valentine, is attached hereto as *Exhibit B*.

9 38. In signing the Certification, Valentine confirmed that he was bound by the
10 Valentine Agreement. He indicated in his own handwriting that he was leaving Fortinet to
11 become the “SVP WW Sales” at “Sophos.” He also reiterated his promise not to solicit any
12 Fortinet employees to leave Fortinet for a period of 12 months following his own termination at
13 Fortinet. From Valentine’s Certification:

14 I also agree that for twelve (12) months from this date, I will not
15 directly or indirectly solicit, induce, recruit or encourage any of the
Company’s employees to leave their employment

16 After leaving the Company’s employment, I would be employed by
17 SOPHOS in the position of: SVP WW Sales.

18 See Exhibit B.

19 **Jason Clark’s Tenure at Fortinet**

20 39. For a period of almost ten years—from March 2004 until recently—Clark served as
21 an officer and senior executive at Fortinet. His title at Fortinet was “Vice President - Systems
22 Engineering.” As an officer and executive of Fortinet, and as the Vice President of Systems
23 Engineering, Clark had substantial managerial responsibilities.

24 40. When Clark began his duties at Fortinet, in exchange for good and valuable
25 consideration, he chose to execute a written agreement (“Clark Agreement”) with Fortinet. Clark
26 chose to sign the Agreement on March 11, 2004. A copy of the Agreement, signed by Clark, is
27 attached hereto as *Exhibit C*.

1 41. In executing the Clark Agreement on March 11, 2004, Clark agreed to a clause
2 with the title “Additional Activities.” Clark agreed as follows:

3 I agree further that for the period of my employment by the
4 Company and for one (1) year after the date of termination of my
5 employment by the Company, I will not (i) induce any employee of
6 the Company to leave the employ of the Company, or (ii) solicit
business of any client or customer of the Company (other than on
behalf of the Company).

7 See Exhibit C at ¶ 7.

8 42. In executing the Clark Agreement on March 11, 2004, Clark also agreed to a clause
9 with the title “Recognition of Company’s Rights; Nondisclosure.” Clark agreed, *inter alia*, that
10 “[a]t all times during the term of my employment and thereafter, I will hold in strictest confidence
11 and will not disclose, use . . . any of the Company’s Proprietary Information . . .” See Exhibit C
12 at ¶ 1.

13 43. In executing the Clark Agreement on March 11, 2004, Clark also agreed to a clause
14 with the title “Return of Company Documents & Equipment.” Clark agreed as follows:

15 Prior to leaving, I will cooperate with the Company in completing
16 and signing the Company’s termination statement for technical and
management personnel.

17 See Exhibit C at ¶ 10.

18 44. Clark chose to leave Fortinet in November 2013.

19 45. When Clark chose to leave Fortinet in November 2013, he *refused* to abide by the
20 requirement in the Clark Agreement that he execute a Certification.

21 **Sophos, Valentine, and Clark Induce Numerous Fortinet Employees to Terminate Their**
22 **Relationships With Fortinet, and Solicit Others to Do the Same**

23 46. Valentine joined Sophos as the “Senior Vice President, Worldwide Sales” in
24 February 2013.

25 47. Valentine—at the intentional direction and/or encouragement and/or request of
26 Sophos—breached Valentine’s contractual and other lawful duties to Fortinet by misusing
27 confidential and trade secret information of Fortinet, including to assist efforts to solicit and
28

1 induce numerous Fortinet employees to leave Fortinet. On information and belief, this unlawful
2 solicitation occurred both before and after Valentine resigned from Fortinet.

3 48. Valentine's misuse of Fortinet information and unlawful solicitation activities are
4 evidenced by numerous facts, including—as examples—the following.

5 49. In April 2013—just two months after Valentine left Fortinet for Sophos—
6 numerous important Fortinet employees, including senior executives, in fact departed Fortinet for
7 Sophos at the inducement of Valentine and Sophos.

8 50. Fortinet's ***Vice President*** of Channel Sales (hereafter, "KK"), left Fortinet for
9 Sophos in April 2013. At Sophos, KK was given the title "Vice President, Channel Sales, North
10 America." KK's "LinkedIn" profile indicates that she now conducts business on behalf of Sophos
11 physically based out of the "Greater Chicago Area."

12 51. Fortinet's ***Vice President*** of Distribution for North America (hereafter, "RG"), also
13 left Fortinet for Sophos in April 2013. At Sophos, RG was given the title "Director of
14 Distribution, North America." RG's "LinkedIn" profile indicates he now conducts business on
15 behalf of Sophos physically based out of "Orange County, California."

16 52. A "Distribution Account Manager" at Fortinet (hereafter, "CB") also left Fortinet
17 for Sophos in April 2013. At Sophos, CB was given the title "Channel Account Executive." CB's
18 "LinkedIn" profile indicates that he now conducts business on behalf of Sophos physically based
19 out of the "Greater Denver Area."

20 53. Not coincidentally, KK, RG, and CB all resigned from Fortinet—to join Valentine
21 at Sophos—in the exact same week of April 2013. Those three employees resigned from Fortinet
22 just a few days shy of two months after Valentine left Fortinet.

23 54. Fortinet's "Director, Central Region Channel Sales" (hereafter, "DD") left Fortinet
24 for Sophos in October 2013. At Sophos, DD was given the title "Director of Central Region
25 Channel Sales." DD's "LinkedIn" profile indicates that he now conducts business on behalf of
26 Sophos physically based out of the "Dallas/Fort Worth Area."

27 55. Clark, Fortinet's former ***Vice President*** – Systems Engineering, left Fortinet for
28 Sophos in November 2013. On information and belief, this followed an in-person meal and/or

1 meeting between Clark, Valentine, and KK in approximately August 2013, after Valentine and KK
2 had left Fortinet.

3 56. On information and belief, Valentine and Clark and Sophos solicited numerous
4 Fortinet employees to leave Fortinet less than 12 months after Valentine and Clark (respectively)
5 left the company. Valentine and Clark and Sophos did this to damage Fortinet, to diminish
6 Fortinet's position in the marketplace, and to unfairly enhance their own positions.

7 57. On information and belief, Sophos and Valentine and/or Clark furthermore induced
8 other former Fortinet employees to violate their agreements with Fortinet by inducing them to
9 solicit other Fortinet employees to leave the company. KK, RG, CB, and DD all signed an
10 agreement—just as Valentine and Clark did—requiring them as a contractual matter not to solicit
11 other employees to leave Fortinet within 12 months of their employment at Fortinet. And yet, on
12 information and belief, KK, RG, CB, and/or DD have solicited Fortinet employees (including each
13 other) to leave the employment of Fortinet.

14 58. Since Clark left Fortinet less than two months ago, the attempts by Sophos and
15 Clark to solicit Fortinet employees to leave Fortinet have increased all the more.

16 59. Shortly after Clark left Fortinet just over a month ago, *four* "Systems Engineers" at
17 Fortinet terminated or announced termination of their employment at Fortinet, and have since
18 joined or announced their intention to join Sophos. It cannot be a coincidence that Clark as the
19 former Vice President of Systems Engineering at Fortinet was followed by four Fortinet Systems
20 Engineers (these Systems Engineers are referred to as "CS"; "JA"; "BE"; and "RA") so quickly.
21 On information and belief, Sophos and Clark worked together, violated Clark's Agreement with
22 Fortinet, and solicited these individuals to leave Fortinet.

23 60. On information and belief, Sophos and Clark worked together, violated Clark's
24 Agreement with Fortinet, and solicited CS, JA, BE, and RA to leave Fortinet.

25 61. On information and belief, Sophos and Valentine and/or Clark furthermore induced
26 CS, JA, BE and RA to violate their own agreements with Fortinet by inducing them to solicit other
27 Fortinet employees to leave Fortinet. CS, JA, BE, and RA all signed an agreement—just as
28 Valentine and Clark did—requiring them as a contractual matter not to solicit other employees to

1 leave Fortinet within 12 months of their employment at Fortinet. And yet, on information and
2 belief, CS, JA, BE, and/or RA have solicited Fortinet employees (including each other) to leave
3 the employment of Fortinet.

4 **The Conduct of Sophos, Valentine, and Clark Is Even Worse Than The Public Changes In**
5 **Employee Status Would Suggest, And Has Gotten Even Worse Since the Initial Complaint**
6 **Was Filed**

7 62. Fortinet filed its initial complaint in this case on December 16, 2013, complaining
8 of much of the conduct alleged herein. In response, Sophos' efforts became more brazen.
9 Furthermore, the conduct of Sophos, Valentine, and/or Clark has been more pervasive than public
10 changes in employee status would suggest; viz., numerous Fortinet employees have been solicited
11 to leave Fortinet, albeit unsuccessfully.

12 63. In or around January–April 2013, Sophos attempted to solicit another of Fortinet's
13 highest ranking *Vice Presidents* to leave Fortinet. On information and belief, this included the
14 participation of Valentine to solicit that Vice President to leave.

15 64. Yet *another Fortinet Vice President*—Fortinet's Vice President of Marketing—
16 has recently been approached many times over by intermediaries used by Sophos, in attempts to
17 solicit him to terminate his employment with Fortinet. The most recent of those attempts to solicit
18 Fortinet's Vice President of Marketing to leave Fortinet occurred on December 17, 2013—the day
19 after Fortinet filed the initial complaint.

20 65. In late November 2013—while still employed at Fortinet—JC wrote a message to
21 another Fortinet employee (“BS”) in which he wrote in part: “As of next week I will be at Sophos
22 working on building an SE team over there. They have some interesting things going on with
23 their products that I think is [sic] very compelling. You, of course, already know a few good
24 people over there already. Hopefully we can indeed work together again in the future. Small
25 industry...”

26 66. Furthermore, in early December 2013, documentary evidence suggests (and
27 Fortinet hereby alleges based on information and belief) that RA was communicating with another
28

1 Fortinet employee (“GM”) regarding the possibility that GM might leave Fortinet as well, in
2 violation of RA’s contractual duties owed to Fortinet.

3 67. Even as of the last week of December, the efforts of Sophos, Valentine, and/or
4 Clark—and other former Fortinet employees—continued. Sophos attempted to convince a
5 Systems Engineer (“DM”) and a sales representative (“RF”) to leave Fortinet as of December
6 27—right on the heels of Fortinet’s initial complaint in this case. On information and belief, Clark
7 was *personally* involved in those solicitation efforts and personally communicated and/or
8 attempted to communicate with at least one of those Fortinet employees.

9 68. Sophos appears intent not just on damaging Fortinet, but furthermore on crowing
10 about it. Clark has recently been broadcasting over Skype to numerous Fortinet employees that
11 “Sophos is hiring.” And Sophos’ CEO responded to Fortinet’s initial complaint by writing a web
12 blog posting in which he referred to this action as “ill-conceived” and “meritless.”

13 69. Sophos’ CEO furthermore recently provided interviews to the press, in which he
14 denigrated this lawsuit.

15 70. Sophos’ attempts—both successful and unsuccessful—to solicit so many Fortinet
16 executives and employees to leave Fortinet was recently (in early December) remarked upon by a
17 Fortinet employee, who sent a note to JA in which the employee wrote in part “Sophos is hiring
18 our whole channel team!” JA responded in part: “Yup, it’s true.”

19 **Misappropriation of Fortinet’s Trade Secrets**

20 71. The individuals who left Fortinet for Sophos received and acquired—while
21 employed by Fortinet—intimate knowledge of, and were otherwise privy to, highly sensitive and
22 valuable trade secret information belonging to Fortinet. This includes valuable, confidential, trade
23 secret information such as:

- 24 (i) information and compilations of information about Fortinet’s customers and
25 customer relationships (including lists, contact information, identity of key
26 decision-makers, historical sales data and purchasing information, sales trends,
27 customer forecasts, customer preferences, customer needs, customer financials,
28 customer leads);

- 1 (ii) information and compilations of information about Fortinet’s potential customers
2 and potential customer relationships (including lists, contact information, identity
3 of key decision-makers, historical sales data and purchasing information from
4 Fortinet or others, sales trends, potential customer forecasts, potential customer
5 preferences, potential customer needs, potential customer financials, potential
6 customer leads);
- 7 (iii) information and compilations of information about Fortinet’s partners, distributors,
8 wholesalers, value-added re-sellers, and downstream companies in the sales
9 channel (including lists, contact information, identity of key decision-makers,
10 financials, historical sales, and forecasts);
- 11 (iv) non-public information and compilations of information about Fortinet products
12 (including business plans, product characteristics, marketing information, sales
13 histories, sales forecasts, product plans, pricing information, tests, competitive
14 intelligence);
- 15 (v) proprietary and confidential information and compilations of information about
16 Fortinet’s workforce (including compilations of names, titles, compensation
17 information, benefits, contact information, application information, employee
18 preferences, employee responsibilities, employee skill-sets, employee performance,
19 employee knowledge and (e.g.) individual employee relationships with actual or
20 potential customers);
- 21 (vi) proprietary and confidential information and compilations of information about
22 how Fortinet markets its products versus Sophos products to partners, distributors,
23 wholesalers, value-added re-sellers, downstream companies in the sales channel,
24 and customers; and
- 25 (vii) other information (i-vii collectively, and with additional details provided below, the
26 “Fortinet Trade Secret(s)”).

27 72. When they left Fortinet for Sophos, Valentine and/or Clark and/or the additional
28 individuals successfully solicited to leave Fortinet (by Sophos, Valentine, and/or Clark, and other

1 former Fortinet employees participating in the solicitation campaign) illegally took these valuable
2 Fortinet Trade Secrets with them.

3 73. The Fortinet Trade Secrets have substantial economic value to Fortinet, including
4 by virtue of the confidential nature of the information. Fortinet has invested large sums to create,
5 update and maintain this information. Fortinet derives substantial economic value and competitive
6 advantages from the Fortinet Trade Secrets. Fortinet would be harmed—and a competitor would
7 derive value—if a competitor learned of Fortinet’s Trade Secrets.

8 74. At all relevant times, Fortinet took reasonable and necessary precautions to guard
9 the secrecy and safety of the Fortinet Trade Secrets. Fortinet protects its facilities, servers,
10 computers, networks, databases, and communications systems using a variety of physical and
11 electronic security systems, such as access cards, password protection systems, firewalls, and
12 encrypted communications technology. Fortinet also requires its employees to read, acknowledge,
13 and sign both an employment agreement and a proprietary information and inventions agreement
14 swearing them to secrecy and loyalty.

15 75. The employment agreements used by Fortinet explicitly inform all employees that
16 Fortinet’s “proprietary information is extremely important” and that an individual’s employment is
17 “expressly subject to your executing a Proprietary Information and Inventions Agreement.” The
18 individuals who departed Fortinet for Sophos thus executed a Proprietary Information and
19 Inventions Agreement (or its equivalent, depending on the time period) and agreed that: “At all
20 times during the term of my employment and thereafter, I will hold in strictest confidence and will
21 not disclose, use, lecture upon or publish any of the Company’s Proprietary Information,” which
22 includes, among other information, “information regarding plans for research, development, new
23 products, marketing and selling, business plans, budgets and unpublished financial statements,
24 licenses, prices and costs, suppliers and customers; and information regarding the skills and
25 compensation of other employees of the Company.”

26 76. These individuals also agreed “that for the period of my employment by the
27 Company and for one (1) year after the date of termination of my employment by the Company, I
28 will not (i) induce any employee of the Company to leave the employ of the Company or (ii)

1 solicit business of any client or customer of the Company (other than on behalf of the Company),”
2 or the equivalent thereto.

3 77. Despite their contractual obligations to Fortinet and other protective safeguards for
4 Fortinet’s sensitive intellectual property, these individuals worked with Sophos, a Fortinet
5 competitor, while employed by Fortinet and thereafter, and failed to disclose that work to Fortinet.
6 While the individuals were employed by Fortinet (and thereafter), they misappropriated and
7 misused Fortinet property and Fortinet resources and Fortinet Trade Secrets for the benefit of
8 themselves and Sophos, and thereby breached their obligations to Fortinet.

9 78. On information and belief, Sophos willfully engaged in a systematic campaign to
10 solicit Fortinet employees to leave Fortinet, and to solicit those employees to disclose Fortinet
11 Trade Secrets to Sophos, in order to illegally acquire and improperly enrich itself from the Fortinet
12 Trade Secrets. Sophos since has used and benefited from the Fortinet Trade Secrets without
13 permission from or compensation to Fortinet.

14 79. Examples of Sophos’ misappropriation of Fortinet Trade Secrets and evidence
15 supporting allegations of that misappropriation are plentiful, although Fortinet expects that
16 substantial additional evidence will come to light during this case.

17 80. **Example 1:** Sophos has improperly acquired and used Fortinet Trade Secret
18 information about Fortinet’s own employees—compilations of information regarding employees’
19 salary and compensation, benefits, responsibilities, titles, skill-sets, customer and distributor
20 relationships, contact information, employment preferences—in its ongoing efforts to convince
21 numerous Fortinet employees to leave Fortinet, to the detriment of Fortinet and to the benefit of
22 Sophos. This includes efforts by Sophos (both successful and unsuccessful) to solicit Valentine (a
23 Fortinet Vice President), Clark (a Fortinet Vice President), KK (a Fortinet Vice President), RG (a
24 Fortinet Vice President), CB, DD, CS, JA, BE, RA, DM, RF, Fortinet’s Vice President –
25 Marketing, and yet another Fortinet Vice President to leave Fortinet. This solicitation activity has
26 been bolstered by Sophos’ improper use of Fortinet Trade Secrets.

27 81. **Example 2:** When employed at Fortinet, RG and CB had access to, and on
28 information and belief acquired, Fortinet Trade Secret information about one of Fortinet’s key

1 partners and distributors (“PA Distributor”). And yet within less than two months of their
2 departure from Fortinet for Sophos, while employed at Sophos, RG and CB were asked by Sophos
3 to work with the PA Distributor to further Sophos’ actual or potential relationship with PA
4 Distributor. In doing so, on information and belief, RG and CB used Fortinet Trade Secrets for
5 the benefit of and at the request of Sophos. This is an example of Sophos using former Fortinet
6 employees, relying on use of Fortinet Trade Secrets, for the benefit of Sophos and the detriment of
7 Fortinet.

8 82. **Example 3:** Numerous Fortinet employees—who were solicited to leave Fortinet,
9 and then joined Sophos—had access to and acquired Fortinet Trade Secret information regarding
10 comparisons (such as but not limited to performance and price comparisons) between Fortinet
11 versus Sophos product and service offerings. For example, in his closing weeks with Fortinet, CS
12 was asked to perform a comparative analysis between Fortinet and Sophos products for a
13 distributor and partner (“TX Distributor”). On information and belief, CS took that Fortinet Trade
14 Secret information to Sophos, and has in fact used that information to further Sophos’ actual or
15 potential relationship with TX Distributor and to harm Fortinet’s relationship with TX Distributor.

16 83. **Example 4:** When JA was employed by Fortinet, he had access to and acquired
17 substantial Fortinet Trade Secret information about a large and vitally important partner,
18 distributor and value-added re-seller for Fortinet (“C Partner”). On JA’s second-to-last day while
19 employed by Fortinet—before moving to Sophos—JA wrote openly with a representative of C
20 Partner about his excitement to work with C Partner, on behalf of Sophos, including anticipated
21 efforts to “differentiate” Sophos offerings from Fortinet offerings. As JA wrote directly to C
22 Partner:

23 I look forward to working with you (and the team) to figure out how to best-
24 position their portfolio going forward. I have several ideas as to things we might
25 be able to do (maybe with our [Sophos’] cloud managed services) to differentiate
26 ourselves from the pack [such as Fortinet]. I’ll def get into it more with you after
27 I make the move [to Sophos].
28

1 On information and belief, JA did in fact join Sophos, and he did in fact—at the knowing request
2 of Sophos—use Fortinet Trade Secret information to improve Sophos’ relationship with C Partner,
3 and to injure Fortinet’s relationship with C Partner.

4 84. **Example 5:** That same day—JA’s second-to-last day at Fortinet—he received a
5 communication from yet another representative of C Partner. That representative wrote to JA as
6 follows:

7 It looks like we will be working with each other come January [once JA joined
8 Sophos]. I wanted to introduce myself since I am the new Sophos Partner
Specialist here [at C Partner].

9 85. JA responded—using his Fortinet email account—to C Partner in part as follows:
10 “I’m looking forward to joining the Sophos team and I’m confident that great things are in store
11 for all of us. My start date [at Sophos] is Jan 6th and I plan on being regularly onsite at [C Partner]
12 shortly after that.”

13 86. Not only did Sophos use JA’s knowledge of Fortinet Trade Secret information
14 about C Partner to its own benefit, Sophos even successfully enticed JA to start that process before
15 JA had even left Fortinet. JA and C Partner were—using Fortinet’s email system—planning for
16 JA to transition his relationship with C Partner from Fortinet to Sophos, using Fortinet Trade
17 Secret information about C Partner, including its own customers, preferences, *et cetera*.

18 87. **Example 6:** In early April 2013—less than 10 days before KK left Fortinet—KK
19 and DD exchanged messages about how to position Fortinet versus Sophos products for a
20 particular Fortinet partner and/or customer, including with a reliance on Fortinet Trade Secret
21 information. On information and belief, KK took that Fortinet Trade Secret information to
22 Sophos, at Sophos’ knowing and intentional request, to use for Sophos’ benefit and Fortinet’s
23 detriment by improving Sophos’ relationship with (and therefore sales or the possibility of sales)
24 the partner and/or customer.

25 88. This scenario of trade secret misappropriation has not been unique. For example,
26 DD, JA, and CS, among others, developed a habit of accessing and circulating Fortinet Trade
27 Secret information shortly before (respectively) leaving Fortinet, including information about
28

1 specific Fortinet customers and partners, product pricing, discounts being offered, margin
2 information for specific sales, and marketing efforts drawing distinctions between Fortinet and
3 Sophos products.

4 89. **Example 7:** On information and belief, numerous individuals who have left
5 Fortinet for Sophos have taken with them, to Sophos, Fortinet Trade Secrets maintained in a
6 confidential and secure data repository hosted by Salesforce.com (“Salesforce Database”). The
7 Salesforce Database contains unique, proprietary Fortinet information considered to be the “crown
8 jewels” of Fortinet’s sales team. The Salesforce Database maintains information such as (i) lists
9 of all the Fortinet customer accounts; (ii) billing addresses, shipping addresses, contact
10 information, emails, telephone numbers, contracts, and contact history; (ii) specific customer,
11 distributor, and partner contact information including titles, telephone numbers, email addresses,
12 “if primary” contact, and other certification information; (iv) an “opportunities” page with details
13 about what various account(s) are looking to buy, product lists, sales stage history, and leads (new,
14 current, or future customers); (v) “special pricing requests” which shows Fortinet products and
15 how much of a discount may have been given, who the distributor was, and how much margin the
16 distributor made, among other information; and (vi) forecasts, dashboards, and reports, through
17 which sales representatives or managers are able to view forecasts and run sales reports.

18 90. To access the Salesforce Database, a Fortinet employee first must be pre-approved
19 and granted access by a Fortinet system administrator; this includes having a personal account
20 created with a unique user name and private password. Accounts to Fortinet’s Salesforce
21 Database are limited and controlled by Fortinet—only employees who have a “need to know” are
22 given access due to the highly sensitive, valuable Fortinet information contained in the database.

23 91. Knowing that much of Fortinet’s most sensitive, valuable sales information resided
24 in the Salesforce Database, in the days and weeks leading up to their respective departures from
25 Fortinet to Sophos, numerous individuals who left Fortinet for Sophos accessed the Salesforce
26 Database at higher-than-normal frequencies in order to steal Fortinet Trade Secrets related to
27 Fortinet sales, leads, customers (current and future), distributors, pricing, and other confidential
28 sales information. As just one example: the individual referred to herein as DD accessed the

1 Salesforce Database numerous times on his very last day with Fortinet—the most recent such
2 access occurring after 3:30 p.m. on his last day at Fortinet. Indeed, DD accessed the SalesForce
3 Database 20 times in his last five days with Fortinet, including on multiple machines (with
4 multiple IP addresses, and multiple browsers and platforms). Log data indicates that DD’s activity
5 on the Salesforce Database ended at 11:59 p.m. on his last day of employment with Fortinet.

6 92. Similarly, while Clark’s last day with Fortinet was November 27, 2013, the day
7 before—November 26—Clark suspiciously accessed the Salesforce Database at 7:00 a.m. in the
8 morning. Prior to that access by Clark—at 7:00 a.m. on his second-to-last day at Fortinet—he had
9 not accessed the Salesforce Database in his usual scope of employment for almost a full month.

10 **Fortinet Versus Sophos Products**

11 93. Because Fortinet and Sophos are competitors, Sophos’ campaign to infringe
12 Fortinet patents, misuse Fortinet trade secrets, and deprive Fortinet of its contractual, statutory and
13 common-law entitlements is aimed at and, on information and belief, has had the effect of hurting
14 Fortinet’s development, marketing, and sales of its own products, and benefitting the
15 development, marketing and sales of Sophos’ products. As such, determining liability and
16 damages for the conduct of Sophos and Valentine and Clark alleged herein will require an inquiry
17 into Sophos’ development, marketing efforts and sales of competing products, including those
18 accused of patent infringement.

19 **COUNT NO. I (Against Sophos)**

20 **INFRINGEMENT OF U.S. PATENT NO. 7,698,744**

21 94. Fortinet realleges and incorporates herein by reference the allegations contained in
22 the preceding paragraphs.

23 95. United States Patent No. 7,698,744 (“the ‘744 patent”), titled “SECURE SYSTEM
24 FOR ALLOWING THE EXECUTION OF AUTHORIZED COMPUTER PROGRAM CODE,”
25 issued on April 13, 2010. A true and correct copy of the ‘744 patent is attached as *Exhibit D* to
26 this First Amended Complaint.

27 96. Fortinet owns all right, title, and interest in and to the ‘744 patent, including all
28 rights to enforce the ‘744 patent.

1 97. On information and belief, without a license or permission from Fortinet, Sophos
2 has infringed and continues to infringe, induced others to infringe and continues to induce others
3 to infringe, and/or has committed and continues to commit acts of contributory infringement,
4 literally or under the doctrine of equivalents, of one or more claims of the ‘744 patent, including at
5 least claim 8 of the ‘744 patent. Sophos’ infringing activities in the United States and in this
6 District include importing, making, using, offering to sell, and/or selling products and devices that
7 embody and/or practice the patented invention, including but not limited to Sophos Anti-Virus
8 software which, on information and belief, is incorporated into, sold with, and/or used with
9 infringing products marketed and/or sold under the names Sophos Enduser Protection Suites,
10 Sophos Endpoint Security and Control, Sophos Endpoint Anti-Virus, Sophos Cloud, and other
11 Sophos products, and contributing to, and inducing consumers and users to make and use the
12 patented invention and to practice the claimed methods.

13 98. Specifically, on information and belief, Sophos induces others, including its
14 customers and end-users, to infringe at least claim 8 of the ‘744 patent by encouraging and
15 facilitating them to perform actions known by Sophos to infringe and with the intent that
16 performance of the actions will infringe. Sophos has been aware of the ‘744 patent since at least
17 December 2013.

18 99. On information and belief, Sophos induces consumers, including its customers and
19 end-users, to make and use the claimed inventions and to practice the claimed methods by (i)
20 providing Sophos Anti-Virus software and (ii) instructing consumers to use Sophos Anti-Virus
21 software along with, *inter alia*, its anti-virus capabilities and in conjunction with Sophos Cloud
22 and/or SophosLabs such that the combination as intended practices each of the elements of at least
23 claim 8 of the ‘744 patent.

24 100. On information and belief, consumers make and use the claimed inventions and
25 practice the claimed methods by using Sophos products, including but not limited to those
26 identified above, that incorporate Sophos Anti-Virus software along with Sophos Cloud and/or
27 SophosLabs, thereby directly infringing at least claim 8 of the ‘744 patent.

101. Sophos also contributes to the infringement of the ‘744 patent because Sophos knows that its products are made for use in an infringing manner and are not staple articles of commerce suitable for substantial non-infringing uses. Sophos’ products, including those enumerated above, which it sells directly to consumers as well as through its distribution partners, are designed to be used (and are used by consumers and end-users) in an infringing manner. Additionally, on information and belief, Sophos’ products, including those identified above, are especially designed, made, or adapted for use in an infringing manner. Sophos’ products have no substantial non-infringing uses and are material to the claimed inventions.

102. On information and belief, Sophos' direct, induced, and/or contributory infringement of the '744 patent has caused and continues to cause substantial damage to Fortinet.

COUNT NO. II (Against Sophos)

INFRINGEMENT OF U.S. PATENT NO. 8,069,487

103. Fortinet realleges and incorporates herein by reference the allegations contained in the preceding paragraphs.

104. United States Patent No. 8,069,487 (“the ‘487 patent”), titled “CLOUD-BASED APPLICATION WHITELISTING,” issued on November 29, 2011. A true and correct copy of the ‘487 patent is attached as ***Exhibit E*** to this First Amended Complaint.

105. Fortinet owns all right, title, and interest in and to the ‘487 patent, including all rights to enforce the ‘487 patent.

106. On information and belief, without a license or permission from Fortinet, Sophos has infringed and continues to infringe, induced others to infringe and continues to induce others to infringe, and/or has committed and continues to commit acts of contributory infringement, literally or under the doctrine of equivalents, of one or more claims of the '487 patent, including at least claim 24 of the '487 patent. Sophos' infringing activities in the United States and in this District include importing, making, using, offering to sell, and/or selling products and devices that embody and/or practice the patented invention, including but not limited to Sophos Anti-Virus software which, on information and belief, is incorporated into, sold with, and/or used with infringing products marketed and/or sold under the names Sophos Enduser Protection Suites,

1 Sophos Endpoint Security and Control, Sophos Endpoint Anti-Virus, Sophos Cloud, among other
2 Sophos products, and contributing to, and inducing consumers and users to make and use the
3 patented invention and to practice the claimed methods.

4 107. Specifically, on information and belief, Sophos induces others, including its
5 customers and end-users, to infringe at least claim 24 of the '487 patent by encouraging and
6 facilitating them to perform actions known by Sophos to infringe and with the intent that
7 performance of the actions will infringe. Sophos has been aware of the '487 patent since at least
8 December 2013.

9 108. On information and belief, Sophos induces consumers, including its customers and
10 end-users, to make and use the claimed inventions and to practice the claimed methods by (i)
11 providing Sophos Anti-Virus software and (ii) instructing consumers to use Sophos Anti-Virus
12 software along with, *inter alia*, its anti-virus capabilities and in conjunction with Sophos Cloud
13 and/or SophosLabs such that the combination as intended practices each of the elements of at least
14 claim 24 of the '487 patent.

15 109. On information and belief, consumers make and use the claimed inventions and
16 practice the claimed methods by using Sophos products, including but not limited to those
17 identified above, that incorporate Sophos Anti-Virus software along with Sophos Cloud and/or
18 SophosLabs, thereby directly infringing at least claim 24 of the '487 patent.

19 110. Sophos also contributes to the infringement of the '487 patent because Sophos
20 knows that its products are made for use in an infringing manner and are not staple articles of
21 commerce suitable for substantial non-infringing uses. Sophos' products, including those
22 enumerated above, which it sells directly to consumers as well as through its distribution partners,
23 are designed to be used (and are used by consumers and end-users) in an infringing manner.
24 Additionally, on information and belief, Sophos' products, including those identified above, are
25 especially designed, made, or adapted for use in an infringing manner. Sophos' products have no
26 substantial non-infringing uses and are material to the claimed inventions.

27 111. On information and belief, Sophos' direct, induced and/or contributory
28 infringement of the '487 patent has caused and continues to cause substantial damage to Fortinet.

1 **COUNT NO. III (Against Sophos)**

2 **INFRINGEMENT OF U.S. PATENT NO. 8,195,938**

3 112. Fortinet realleges and incorporates herein by reference the allegations contained in
4 the preceding paragraphs.

5 113. United States Patent No. 8,195,938 (“the ‘938 patent”), titled “CLOUD-BASED
6 APPLICATION WHITELISTING,” issued on June 5, 2012. A true and correct copy of the ‘938
7 patent is attached as *Exhibit F* to this First Amended Complaint.

8 114. Fortinet owns all right, title, and interest in and to the ‘938 patent, including all
9 rights to enforce the ‘938 patent.

10 115. On information and belief, without a license or permission from Fortinet, Sophos
11 has infringed and continues to infringe, induced others to infringe and continues to induce others
12 to infringe, and/or has committed and continues to commit acts of contributory infringement,
13 literally or under the doctrine of equivalents, of one or more claims of the ‘938 patent, including at
14 least claim 30 of the ‘938 patent. Sophos’ infringing activities in the United States and in this
15 District include importing, making, using, offering to sell, and/or selling products and devices that
16 embody and/or practice the patented invention, including but not limited to Sophos Anti-Virus
17 software which, on information and belief, is incorporated into, sold with, and/or used with
18 infringing products marketed and/or sold under the names Sophos Enduser Protection Suites,
19 Sophos Endpoint Security and Control, Sophos Endpoint Anti-Virus, Sophos Cloud, among other
20 Sophos products, and contributing to, and inducing consumers and users to make and use the
21 patented invention and to practice the claimed methods.

22 116. Specifically, on information and belief, Sophos induces others, including its
23 customers and end-users, to infringe at least claim 30 of the ‘938 patent by encouraging and
24 facilitating them to perform actions known by Sophos to infringe and with the intent that
25 performance of the actions will infringe. Sophos has been aware of the ‘938 patent since at least
26 December 2013.

27 117. On information and belief, Sophos induces consumers, including its customers and
28 end-users, to make and use the claimed inventions and to practice the claimed methods by (i)

1 providing Sophos Anti-Virus software and (ii) instructing consumers to use Sophos Anti-Virus
2 software along with, *inter alia*, its anti-virus capabilities and in conjunction with Sophos Cloud
3 and/or SophosLabs such that the combination as intended practices each of the elements of at least
4 claim 30 of the ‘938 patent.

5 118. On information and belief, consumers make and use the claimed inventions and
6 practice the claimed methods by using Sophos products, including but not limited to those
7 identified above, that incorporate Sophos Anti-Virus software along with Sophos Cloud and/or
8 SophosLabs, thereby directly infringing at least claim 30 of the ‘938 patent.

9 119. Sophos also contributes to the infringement of the ‘938 patent because Sophos
10 knows that its products are made for use in an infringing manner and are not staple articles of
11 commerce suitable for substantial non-infringing uses. Sophos’ products, including those
12 enumerated above, which it sells directly to consumers as well as through its distribution partners,
13 are designed to be used (and are used by consumers and end-users) in an infringing manner.
14 Additionally, on information and belief, Sophos’ products, including those identified above, are
15 especially designed, made, or adapted for use in an infringing manner. Sophos’ products have no
16 substantial non-infringing uses and are material to the claimed inventions.

17 120. On information and belief, Sophos’ direct, induced, and/or contributory
18 infringement of the ‘938 patent has caused and continues to cause substantial damage to Fortinet.

19 **COUNT NO. IV (Against Sophos)**

20 **INFRINGEMENT OF U.S. PATENT NO. 7,333,430**

21 121. Fortinet realleges and incorporates herein by reference the allegations contained in
22 the preceding paragraphs.

23 122. United States Patent No. 7,333,430 (“the ‘430 patent”), titled “SYSTEMS AND
24 METHODS FOR PASSING NETWORK TRAFFIC DATA,” issued on February 19, 2008. A
25 true and correct copy of the ‘430 patent is attached as *Exhibit G* to this First Amended Complaint.

26 123. Fortinet owns all right, title, and interest in and to the ‘430 patent, including all
27 rights to enforce the ‘430 patent.

1 124. On information and belief, without a license or permission from Fortinet, Sophos
2 has infringed and continues to infringe, induced others to infringe and continues to induce others
3 to infringe, and/or has committed and continues to commit acts of contributory infringement,
4 literally or under the doctrine of equivalents, of one or more claims of the ‘430 patent, including at
5 least claim 16 of the ‘430 patent. Sophos’ infringing activities in the United States and in this
6 District include importing, making, using, offering to sell, and/or selling products and devices that
7 embody and/or practice the patented invention, including but not limited to the Sophos Unified
8 Threat Management (UTM) suite of appliances running Sophos’ UTM operating system (“OS”),
9 and contributing to, and inducing consumers and users to make and use the patented invention and
10 to practice the claimed methods.

11 125. Specifically, on information and belief, Sophos induces others, including its
12 customers and end-users, to infringe at least claim 16 of the ‘430 patent by encouraging and
13 facilitating them to perform actions known by Sophos to infringe and with the intent that
14 performance of the actions will infringe. Sophos has been aware of the ‘430 patent since at least
15 the filing of the First Amended Complaint.

16 126. On information and belief, Sophos induces consumers, including its customers and
17 end-users, to make and use the claimed inventions and to practice the claimed methods by
18 configuring the accused Sophos UTM appliances, as intended by Sophos, to practice each of the
19 elements of at least claim 16 of the ‘430 patent.

20 127. On information and belief, consumers make and use the claimed inventions and
21 practice the claimed methods by configuring and using Sophos UTM appliances, including but not
22 limited to those identified above, that incorporate the Sophos UTM OS, thereby directly infringing
23 at least claim 16 of the ‘430 patent.

24 128. Sophos also contributes to the infringement of the ‘430 patent because Sophos
25 knows that its UTM appliances are made for use in an infringing manner and are not staple articles
26 of commerce suitable for substantial non-infringing uses. Sophos’ UTM appliances, which it sells
27 directly to consumers as well as through its distribution partners, are designed to be used (and are
28 used by consumers and end-users) in an infringing manner. Additionally, on information and

1 belief, Sophos' UTM appliances, including those identified above, are especially designed, made,
2 or adapted for use in an infringing manner. Sophos' UTM appliances have no substantial non-
3 infringing uses and are material to the claimed inventions.

4 129. On information and belief, Sophos' direct, induced, and/or contributory
5 infringement of the '430 patent has caused and continues to cause substantial damage to Fortinet.

6 **COUNT NO. V (Against Sophos)**

7 **INFRINGEMENT OF U.S. PATENT NO. 7,376,125**

8 130. Fortinet realleges and incorporates herein by reference the allegations contained in
9 the preceding paragraphs.

10 131. United States Patent No. 7,376,125 ("the '125 patent"), titled "SERVICE
11 PROCESSING SWITCH," issued on May 20, 2008. A true and correct copy of the '125 patent is
12 attached as *Exhibit H* to this First Amended Complaint.

13 132. Fortinet owns all right, title, and interest in and to the '125 patent, including all
14 rights to enforce the '125 patent.

15 133. On information and belief, without a license or permission from Fortinet, Sophos
16 has infringed and continues to infringe, induced others to infringe and continues to induce others
17 to infringe, and/or has committed and continues to commit acts of contributory infringement,
18 literally or under the doctrine of equivalents, of one or more claims of the '125 patent, including at
19 least claim 1 of the '125 patent. Sophos' infringing activities in the United States and in this
20 District include importing, making, using, offering to sell, and/or selling products and devices that
21 embody and/or practice the patented invention, including but not limited to the Sophos Unified
22 Threat Management (UTM) suite of appliances running Sophos' UTM operating system ("OS"),
23 and contributing to, and inducing consumers and users to make and use the patented invention and
24 to practice the claimed methods.

25 134. Specifically, on information and belief, Sophos induces others, including its
26 customers and end-users, to infringe at least claim 1 of the '125 patent by encouraging and
27 facilitating them to perform actions known by Sophos to infringe and with the intent that
28

1 performance of the actions will infringe. Sophos has been aware of the ‘125 patent since at least
2 the filing of the First Amended Complaint.

3 135. On information and belief, Sophos induces consumers, including its customers and
4 end-users, to make and use the claimed inventions and to practice the claimed methods by
5 configuring the accused Sophos UTM appliances, as intended by Sophos, to practice each of the
6 elements of at least claim 1 of the ‘125 patent.

7 136. On information and belief, consumers make and use the claimed inventions and
8 practice the claimed methods by using Sophos UTM appliances that incorporate the Sophos UTM
9 OS, thereby directly infringing at least claim 1 of the ‘125 patent.

10 137. Sophos also contributes to the infringement of the ‘125 patent because Sophos
11 knows that its UTM appliances are made for use in an infringing manner and are not staple articles
12 of commerce suitable for substantial non-infringing uses. Sophos’ UTM appliances, which it
13 sells directly to consumers as well as through its distribution partners, are designed to be used (and
14 are used by consumers and end-users) in an infringing manner. Additionally, on information and
15 belief, Sophos’ UTM appliances, including those identified above, are especially designed, made,
16 or adapted for use in an infringing manner. Sophos’ UTM appliances have no substantial non-
17 infringing uses and are material to the claimed inventions.

18 138. On information and belief, Sophos’ direct, induced, and/or contributory
19 infringement of the ‘125 patent has caused and continues to cause substantial damage to Fortinet.

20 **COUNT NO. VI (Against Sophos)**

21 **INFRINGEMENT OF U.S. PATENT NO. 7,609,625**

22 139. Fortinet realleges and incorporates herein by reference the allegations contained in
23 the preceding paragraphs.

24 140. United States Patent No. 7,609,625 (“the ‘625 patent”), titled “SYSTEMS AND
25 METHODS FOR DETECTING AND PREVENTING FLOODING ATTACKS IN A NETWORK
26 ENVIRONMENT,” issued on October 27, 2009. A true and correct copy of the ‘625 patent is
27 attached as *Exhibit I* to this First Amended Complaint.

1 141. Fortinet owns all right, title, and interest in and to the ‘625 patent, including all
2 rights to enforce the ‘625 patent.

3 142. On information and belief, without a license or permission from Fortinet, Sophos
4 has infringed and continues to infringe, induced others to infringe and continues to induce others
5 to infringe, and/or has committed and continues to commit acts of contributory infringement,
6 literally or under the doctrine of equivalents, of one or more claims of the ‘625 patent, including at
7 least claim 6 of the ‘625 patent. Sophos’ infringing activities in the United States and in this
8 District include importing, making, using, offering to sell, and/or selling products and devices that
9 embody and/or practice the patented invention, including but not limited to the Sophos Unified
10 Threat Management (UTM) suite of appliances running Sophos’ UTM operating system (“OS”),
11 and contributing to, and inducing consumers and users to make and use the patented invention and
12 to practice the claimed methods.

13 143. Specifically, on information and belief, Sophos induces others, including its
14 customers and end-users, to infringe at least claim 6 of the ‘625 patent by encouraging and
15 facilitating them to perform actions known by Sophos to infringe and with the intent that
16 performance of the actions will infringe. Sophos has been aware of the ‘625 patent since at least
17 the filing of the First Amended Complaint.

18 144. On information and belief, Sophos induces consumers, including its customers and
19 end-users, to make and use the claimed inventions and to practice the claimed methods by
20 configuring the accused Sophos UTM appliances, as intended by Sophos, to practice each of the
21 elements of at least claim 6 of the ‘625 patent.

22 145. On information and belief, consumers make and use the claimed inventions and
23 practice the claimed methods by using Sophos products that incorporate the Sophos UTM OS,
24 thereby directly infringing at least claim 6 of the ‘625 patent.

25 146. Sophos also contributes to the infringement of the ‘625 patent because Sophos
26 knows that its UTM appliances are made for use in an infringing manner and are not staple articles
27 of commerce suitable for substantial non-infringing uses. Sophos’ UTM appliances, which it sells
28 directly to consumers as well as through its distribution partners, are designed to be used (and are

1 used by consumers and end-users) in an infringing manner. Additionally, on information and
2 belief, Sophos' UTM appliances are especially designed, made, or adapted for use in an infringing
3 manner. Sophos' UTM appliances have no substantial non-infringing uses and are material to the
4 claimed inventions.

5 147. On information and belief, Sophos' direct, induced, and/or contributory
6 infringement of the '625 patent has caused and continues to cause substantial damage to Fortinet.

7 **COUNT NO. VII (Against Valentine)**

8 **BREACH OF CONTRACT**

9 148. Fortinet realleges and incorporates herein by reference the allegations contained in
10 the preceding paragraphs.

11 149. Fortinet and Valentine entered into a contract, described herein as the Valentine
12 Agreement and attached hereto as Exhibit A.

13 150. Fortinet did all, or substantially all, of the significant things that the Valentine
14 Agreement required it to do, and/or Fortinet was excused from doing those things based on
15 Valentine's breaches of the Valentine Agreement.

16 151. For all conditions required by the Valentine Agreement for Valentine's
17 performance, all such conditions occurred and/or were excused.

18 152. Valentine breached the Valentine Agreement by soliciting, directly and indirectly,
19 and attempting to solicit numerous Fortinet employees to leave Fortinet within 12 months or less
20 of Valentine's termination from Fortinet.

21 153. Valentine furthermore breached the Valentine Agreement by using Fortinet Trade
22 Secrets for his own benefit and for the benefit of Sophos, without permission from Fortinet.

23 154. Fortinet was harmed by these breaches in an amount to be proven at trial.

24 155. Fortinet has been and will be harmed irreparably as a result of Valentine's
25 continued breaches of the Valentine Agreement, unless that conduct is enjoined by this Court.

1 **COUNT NO. VIII (Against Clark)**

2 **BREACH OF CONTRACT**

3 156. Fortinet realleges and incorporates herein by reference the allegations contained in
4 the preceding paragraphs.

5 157. Fortinet and Clark entered into a contract, described herein as the Clark Agreement
6 and attached hereto as Exhibit C.

7 158. Fortinet did all, or substantially all, of the significant things that the Clark
8 Agreement required it to do, and/or Fortinet was excused from doing those things based on
9 Clark's breaches of the Clark Agreement.

10 159. For all conditions required by the Clark Agreement for Clark's performance, all
11 such conditions occurred and/or were excused.

12 160. Clark breached the Clark Agreement by soliciting, directly and indirectly, and
13 attempting to solicit numerous Fortinet employees to leave Fortinet within 12 months or less of
14 Clark's termination from Fortinet.

15 161. Clark furthermore breached the Clark Agreement by using Fortinet Trade Secrets
16 for his own benefit and for the benefit of Sophos, without permission from Fortinet.

17 162. Fortinet was harmed by these breaches in an amount to be proven at trial.

18 163. Fortinet has been and will be harmed irreparably as a result of Clark's continued
19 violations of the Clark Agreement, unless that conduct is enjoined by this Court.

20 **COUNT NO. IX (Against Sophos, Valentine, and Clark)**

21 **INTENTIONAL INTERFERENCE WITH CONTRACT**

22 164. Fortinet realleges and incorporates herein by reference the allegations contained in
23 the preceding paragraphs.

24 165. Fortinet entered into the Valentine Agreement—a valid contract—with Valentine,
25 pursuant to which Valentine agreed not to solicit Fortinet employees to leave Fortinet during a
26 reasonable period of time. Fortinet entered into the Clark Agreement—a valid contract—with
27 Clark, pursuant to which Clark made substantially the same agreement. Likewise, all individuals
28 described above who left Fortinet for Sophos signed an agreement with Fortinet with the same

1 relevant provisions not to solicit Fortinet employees to leave the company for a reasonable period
2 of time.

3 166. Upon information and belief, Sophos became aware of Valentine's Agreement no
4 later than Valentine's decision to accept an offer of employment from Sophos, in or before
5 February 2013. Sophos likewise became aware of the agreements—all containing substantially
6 the same provisions against solicitation of employees away from Fortinet for a reasonable period
7 of time—between Fortinet and all of its employees at the same time, including Clark.

8 167. Upon information and belief, Valentine became aware of the agreements—all
9 containing substantially the same provisions against solicitation of employees away from Fortinet
10 for a reasonable period of time and against use of Fortinet Trade Secrets—between Fortinet and all
11 of its employees, including Clark, during the course of his employment with Fortinet, and, in any
12 case, prior to the termination of his employment with Fortinet in February 2013.

13 168. Upon information and belief, Clark became aware of the agreements—all
14 containing substantially the same provisions against solicitation of employees away from Fortinet
15 for a reasonable period of time and against use of Fortinet Trade Secrets—between Fortinet and all
16 of its employees, during the course of his employment with Fortinet, and, in any case, prior to the
17 termination of his employment with Fortinet in November 2013.

18 169. Upon information and belief, Sophos intentionally induced Valentine to breach the
19 Valentine Agreement by inducing him to solicit Fortinet employees to leave Fortinet both before
20 and shortly after (and less than 12 months from the date that) Valentine terminated his
21 employment with Fortinet.

22 170. Upon information and belief, Sophos and Valentine intentionally induced Clark to
23 breach the Clark Agreement by inducing him to solicit Fortinet employees to leave Fortinet both
24 before and shortly after (and less than 12 months from the date that) Clark terminated his
25 employment with Fortinet.

26 171. Upon information and belief, Sophos and Valentine and/or Clark intentionally
27 induced individual employees who left Fortinet, for Sophos, to breach their written agreements
28 with Fortinet by inducing them to solicit other Fortinet employees to leave Fortinet both before

1 and shortly after (and less than 12 months from the date that) they terminated their employment
2 with Fortinet, including each other.

3 172. Sophos engaged in wrongful conduct by intentionally disrupting Valentine's
4 performance of, and by inducing his breaches of, the Valentine Agreement.

5 173. Sophos and Valentine engaged in wrongful conduct by intentionally disrupting
6 Clark's performance of, and by inducing his breaches of, the Clark Agreement.

7 174. Sophos and Valentine and Clark engaged in wrongful conduct by intentionally
8 disrupting numerous Fortinet employees' performance of, and by inducing their breaches of, their
9 written agreements with Fortinet as described herein.

10 175. The actions of Sophos, Valentine, and Clark identified in this pleading were done
11 with the intention of disrupting the contractual relationships between Fortinet and Valentine,
12 Fortinet and Clark, and between Fortinet and numerous other Fortinet employees.

13 176. The actions of Sophos Valentine and Clark identified in this complaint resulted in
14 numerous breaches of the Valentine Agreement by Valentine, the Clark Agreement by Clark, and
15 other former Fortinet employees' breaches of their respective written contracts with Fortinet.

16 177. As an actual and proximate result of the conduct of Sophos, Valentine, and Clark,
17 Fortinet has been damaged in the amount to be proven at trial.

18 178. The conduct of Sophos, Valentine, and Clark was a substantial factor in causing
19 Fortinet's harm.

20 179. In performing the acts described above, Sophos, Valentine, and Clark acted
21 willfully, maliciously, oppressively, with the intent to interfere with Fortinet's contractual interests
22 and with conscious disregard for Fortinet's rights and the damages it would suffer thereby.

23 **COUNT NO. X (Against Valentine and Clark)**

24 **BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING**

25 180. Fortinet realleges and incorporates herein by reference the allegations contained in
26 the preceding paragraphs.

27 181. The Valentine Agreement and the Clark Agreement both included an implied
28 covenant of good faith and fair dealing between the respective parties. The implied covenant

1 imposed on Valentine and Clark a duty not to do anything to deprive Fortinet of the benefits of the
2 agreements.

3 182. Valentine's conduct, described above, unfairly interfered with Fortinet's right to
4 receive the benefits of the contract, constituting a breach of the implied covenant of good faith and
5 fair dealing.

6 183. Clark's conduct, described above, unfairly interfered with Fortinet's right to receive
7 the benefits of the contract, constituting a breach of the implied covenant of good faith and fair
8 dealing.

9 184. Valentine's and Clark's breaches of the implied covenant of good faith and fair
10 dealing harmed Fortinet in an amount to be proven at trial.

11 **COUNT NO. XI (Against Sophos)**

12 **TRADE SECRET MISAPPROPRIATION**

13 185. Fortinet realleges and incorporates herein by reference the allegations contained in
14 the preceding paragraphs.

15 186. Fortinet owns the Fortinet Trade Secrets, described more fully above, which give
16 Fortinet a significant competitive advantage over its existing and would-be competitors, including
17 Sophos. This advantage, at least as to Sophos, was compromised as a result of Sophos' unlawful
18 activities.

19 187. Fortinet invested substantial resources to develop the Fortinet Trade Secrets. And
20 the Fortinet Trade Secrets derive independent economic value, actual or potential, from not being
21 generally known to the public or to other persons who can obtain economic value from their
22 disclosure or use.

23 188. Fortinet made reasonable efforts under the circumstances to maintain the
24 confidentiality of the Fortinet Trade Secrets. Fortinet's efforts included, but are not limited to, (i)
25 having employees and consultants who may have access to the Fortinet Trade Secrets sign
26 confidentiality agreements that oblige them not to disclose the Fortinet Trade Secrets or
27 characteristics of the Fortinet Trade Secrets; (ii) limiting the circulation of said materials within
28 Fortinet; (iii) protecting, limiting, and controlling access to Fortinet properties with security cards,

1 and other physical or electronic means; (iv) protecting, limiting, and controlling access to
2 computers with secure log-in identifications and passwords; (v) limiting each employee's access
3 to electronic files to those that the particular employee needs to access (*i.e.*, information
4 segregation); (vi) educating employees on the nature of Fortinet's information that is confidential
5 and proprietary; and (vii) reminding employees on a regular and periodic basis of their obligation
6 to protect and maintain Fortinet's confidential and proprietary information.

7 189. Fortinet did not consent to the use of any of the Fortinet Trade Secrets by anyone
8 other than authorized Fortinet employees using them for Fortinet's own business purposes.

9 190. On information and belief, and as described above, certain former Fortinet
10 employees entered into an agreement with Sophos, and/or acted at the request and encouragement
11 of Sophos, whereby they would misappropriate Fortinet Trade Secrets in order to give Sophos an
12 unfair advantage in the network security marketplace.

13 191. On information and belief, certain former Fortinet employees (now Sophos
14 employees) willfully and intentionally misappropriated Fortinet Trade Secrets on Sophos' behalf
15 by acquiring, disclosing, and/or using Fortinet Trade Secrets for Sophos' purposes—for example
16 but not limited to, by soliciting numerous Fortinet employees to leave Fortinet to the detriment of
17 Fortinet and the benefit of Sophos while using Fortinet Trade Secrets and, on information and
18 belief, by using Fortinet Trade Secrets about Fortinet customers, products and partners to improve
19 Sophos' development, marketing, sales and distribution of Sophos products—even though such
20 employees owed a duty to Fortinet to maintain the confidentiality of the Fortinet Trade Secrets,
21 which Sophos knew.

22 192. Sophos has illegally obtained and used Fortinet Trade Secrets as set forth above
23 and through other means of which Fortinet presently is unaware.

24 193. On information and belief, at all times Sophos knew or had reason to know that
25 Fortinet Trade Secrets were obtained from Fortinet by improper means.

26 194. On information and belief, Sophos has used and disclosed Fortinet Trade Secrets
27 without Fortinet's consent and without regard to Fortinet's rights, and without compensation,
28 permission, or licenses for the benefit of themselves and others.

1 195. Sophos' conduct was, is, and remains willful and wanton, and was taken with
2 blatant disregard for Fortinet's valid and enforceable rights.

3 196. Sophos' wrongful conduct has caused and, unless enjoined by this Court, will
4 continue in the future to cause irreparable injury to Fortinet. Fortinet has no adequate remedy at
5 law for such wrongs and injuries. Fortinet is therefore entitled to an injunction restraining and
6 enjoining Sophos and its agents, servants, officers, directors, and employees, and all persons
7 acting there under, in concert with, or on their behalf, from further using in any manner Fortinet
8 Trade Secrets.

9 197. In addition, as a proximate result of Sophos' misconduct, Fortinet has suffered
10 actual damages, and Sophos has been unjustly enriched.

11 198. Sophos' misappropriation of Fortinet Trade Secrets was willful and malicious; on
12 information and belief, Sophos misappropriated Fortinet's Trade Secrets with the deliberate intent
13 to injure Fortinet's business and improve its own. Fortinet is therefore entitled to enhanced
14 damages and reasonable attorneys' fees.

15 **COUNT NO. XII (Against Sophos, Valentine, and Clark)**

16 **CIVIL CONSPIRACY**

17 199. Fortinet realleges and incorporates herein by reference the allegations contained in
18 the preceding paragraphs.

19 200. Sophos, Valentine, and Clark agreed to an ongoing scheme to harm Fortinet in
20 unlawful ways including (for example) widespread, intentional interference with contract and the
21 inside recruitment of Fortinet employees for Sophos.

22 201. Sophos, Valentine, and Clark knew that their conspiracy was unlawful because, for
23 example, their acts constituted interference with Fortinet's contracts and breaches of Valentine's
24 and/or Clark's contractual and fiduciary duties of confidentiality and loyalty, and would harm
25 Fortinet and benefit Sophos in improper ways. They acted in concert and came to a mutual
26 understanding to accomplish a common and unlawful plan to harm Fortinet. They furthermore
27 agreed and intended that the actions of Sophos and Valentine and Clark—for example, to solicit
28

Fortinet employees to leave Fortinet, in violation of the Valentine and Clark Agreements—occur, and they took these actions in furtherance of the conspiracy.

202. As a direct result of this conspiracy, and due to the acts of Sophos and Valentine and Clark (taken separately or together) committed pursuant to this conspiracy, Fortinet has been harmed in an amount to be proven at trial.

203. Sophos’ conspiring in the wrongful acts of Valentine and Clark was willful and malicious and justifies an award of punitive damages.

COUNT NO. XIII (Against Valentine and Clark)

BREACH OF FIDUCIARY DUTY

204. Fortinet realleges and incorporates herein by reference the allegations contained in the preceding paragraphs.

205. By virtue of his employment with Fortinet and his executive officer position at Fortinet as “Vice President Americas - Sales and Support,” as well as pursuant to his written agreements with Fortinet, Valentine occupied a position of trust and confidence with Fortinet. By virtue of his position of trust, Valentine owed fiduciary duties of loyalty and confidentially to Fortinet.

206. By virtue of his employment with Fortinet and his executive officer position at Fortinet as “Vice President - Systems Engineering,” as well as pursuant to his written agreements with Fortinet, Clark occupied a position of trust and confidence with Fortinet. By virtue of his position of trust, Clark owed fiduciary duties of loyalty and confidentially to Fortinet.

207. Despite these duties, Valentine and Clark misused their positions of trust and confidence to further their own interests and those of Sophos, at the expense of Fortinet, and breached their fiduciary duties to Fortinet by engaging in the acts described above, including but not limited to, soliciting Fortinet employees away from Fortinet while they were still serving as executive officers of Fortinet and/or providing inside information to Sophos to facilitate the solicitation of Fortinet employees to leave Fortinet.

208. As a direct and proximate result of Valentine’s and Clark’s breaches of their fiduciary duties, Fortinet has suffered harm in an amount to be proven at trial.

1 209. Valentine's and Clark's breaches of their fiduciary duties were willful and
2 malicious and justify an award of punitive damages.

3 **COUNT NO. XIV (Against Sophos)**

4 **AIDING AND ABETTING BREACH OF FIDUCIARY DUTY**

5 210. Fortinet realleges and incorporates herein by reference the allegations contained in
6 the preceding paragraphs.

7 211. Valentine and Clark each owed a fiduciary duty to Fortinet, which they breached by
8 acting in the manner described above.

9 212. Sophos aided and abetted Valentine's and/or Clark's breaches of their fiduciary
10 duties. Sophos knew that Valentine's and Clark's insider recruitment and solicitation of Fortinet
11 employees to leave Fortinet, as well as their provision of inside information to Sophos to facilitate
12 the ongoing solicitation of Fortinet employees to leave Fortinet, constituted breaches of
13 Valentine's and/or Clark's fiduciary duties. By offering Valentine and Clark financial incentives
14 and/or inducing Valentine and Clark to engage in the acts of solicitation described above, Sophos
15 gave substantial assistance and/or encouragement to Valentine and/or Clark to breach their
16 fiduciary duties.

17 213. As a direct and proximate result of Sophos' aiding and abetting Valentine's and/or
18 Clark's breaches of their fiduciary duties, Fortinet has suffered harm in an amount to be proven at
19 trial.

20 214. Sophos' aiding and abetting Valentine's and/or Clark's breaches of their fiduciary
21 duties was willful and malicious and justifies an award of punitive damages.

22 **COUNT NO. XV (Against Sophos)**

23 **VIOLATION OF CAL. BUS. & PROF. CODE § 17200 ET SEQ.**

24 **UNFAIR COMPETITION**

25 215. Fortinet realleges and incorporates herein by reference the allegations contained in
26 the preceding paragraphs.

27 216. On information and belief, and as described more fully above, Sophos has
28 knowingly performed acts, including but not limited to, intentionally interfering with the contracts

1 Fortinet has with its employees by inducing individual employees to breach their written
2 agreements with Fortinet by inducing them to solicit other Fortinet employees to leave Fortinet
3 both before and shortly after (and less than 12 months from the date that) they terminated their
4 employment with Fortinet, including Valentine and Clark; and aiding and abetting Valentine's
5 and/or Clark's breaches of their fiduciary duties.

6 217. On information and belief, Sophos knowingly committed these acts in order to
7 pirate Fortinet's employee base by interfering with the valid contracts—and the benefits of those
8 contracts—that Fortinet has with its employees, and by substantially assisting and/or encouraging
9 Valentine and/or Clark to commit known breaches of their fiduciary duties by continuing their acts
10 of inside employee solicitation. These acts constitute unlawful, unfair, and/or fraudulent business
11 practices and unfair competition under Sections 17200, *et seq.*, of the California Business and
12 Professions Code.

13 218. As a result of such conduct, Fortinet has suffered, and will continue to suffer,
14 irreparable harm by Sophos' unfair, unlawful and/or fraudulent practices and unfair competition,
15 including but not limited to, harm to its reputation, goodwill, and stature in the business
16 community and with its customers, for which there is no adequate remedy at law, thereby
17 justifying injunctive relief. Until and unless injunctive relief is granted, Sophos will be unjustly
18 enriched, which should be disgorged pursuant to allowable remedies under Sections 17200, *et*
19 *seq.*, of the California Business and Professions Code.

20 **DEMAND FOR JURY TRIAL**

21 219. Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Fortinet demands a
22 jury trial on all triable issues.

23 **PRAYER FOR RELIEF**

24 WHEREFORE, Fortinet prays for judgment and relief as follows:

25 A. A declaration that the Asserted Patents are valid and enforceable, and that Sophos
26 has infringed and continues to infringe one or more claims of the Asserted Patents;

27 B. A declaration that Sophos has violated Fortinet's contractual, common-law and
28 statutory rights, including through intentional interference with contract, trade secret

1 misappropriation, and aiding and abetting breaches of fiduciary duties;

2 C. A declaration that Valentine and/or Clark have breached contracts and implied
3 covenants with Fortinet, and have breached the fiduciary duties owed to Fortinet;

4 D. A declaration that Sophos, Valentine, and Clark have violated Fortinet's
5 contractual, common-law and statutory rights, including in the form of a civil conspiracy, contract
6 breaches, induced breaches of contract, unfair competition, and/or trade secret misappropriation,
7 as described herein;

8 E. A preliminary and/or permanent injunction enjoining Sophos, its directors, officers,
9 agents, and employees, and those acting in privity or in concert with them, including Valentine
10 and Clark, and their partners, subsidiaries, divisions, successors, and assigns, from further acts of
11 (i) interference with Fortinet's contracts, (ii) trade secret misappropriation, (iii) patent
12 infringement, contributory patent infringement, and/or inducement of patent infringement of the
13 Asserted Patents, and (iv) unfair competition;

14 F. An award of damages adequate to compensate Fortinet for Sophos' patent
15 infringement, in accordance with 35 U.S.C. § 284, including all pre-judgment and post-judgment
16 interest and costs;

17 G. Increasing the patent damages to three times the amount found or assessed by
18 virtue of the deliberate and willful nature of Sophos' infringement, in accordance with 35 U.S.C. §
19 284;

20 H. A judgment that this is an exceptional case and that Fortinet be awarded attorneys'
21 fees under 35 U.S.C. § 285;

22 I. A judgment that Fortinet be awarded damages as a result of Sophos' intentional
23 interference with Fortinet's contracts;

24 J. A judgment that Fortinet be awarded damages as a result of Valentine's and Clark's
25 intentional interference with Fortinet's contracts;

26 K. A judgment that Fortinet be awarded damages as a result of Valentine's and Clark's
27 breaches of contract and implied covenants of good faith and fair dealing;

28 L. A judgment that Fortinet be awarded damages as a result of Valentine's and Clark's

1 breaches of their fiduciary duties;

2 M. A judgment that Fortinet be awarded damages as a result of Sophos' aiding and
3 abetting Valentine's and/or Clark's breaches of their fiduciary duties;

4 N. A judgment that Fortinet be awarded damages as a result of Sophos' trade secret
5 misappropriation, and enhanced damages pursuant to Sophos' willful and malicious conduct;

6 O. A judgment that Fortinet be awarded attorneys' fees and costs pursuant to Cal.
7 Civil Code Section 3426.4;

8 P. A judgment that Fortinet be awarded punitive damages;

9 Q. A judgment that Fortinet be awarded pre-judgment and post-judgment interest on
10 any award;

11 R. A judgment that Fortinet be awarded other relief including but not limited to
12 disgorgement of any amounts by which Sophos, Valentine, and/or Clark have been unjustly
13 enriched as a result of their wrongful conduct; and

14 S. That the Court award Fortinet any other relief as the Court deems just and proper.
15

16 Dated: January 9, 2014

Respectfully submitted,

17
18 By: /s/John M. Neukom

19 JOHN M. NEUKOM (CA Bar No. 275887)
johnneukom@quinnemanuel.com
20 QUINN EMANUEL URQUHART & SULLIVAN,
LLP
50 California Street, 22nd Floor
21 San Francisco, California 94111
Telephone: (415) 875-6600
22 Facsimile: (415) 875-6700

23 Attorneys for Plaintiff FORTINET, INC.
24
25
26
27
28